

ABSTRACT

A novel and useful apparatus for and method of securely downloading and installing a patch program in a processing device. Each processing device is assigned a unique key embedded therein during manufacture and has knowledge of a shared key. The program patch is encrypted using the shared key and transmitted over a communication link to each device. The patch is decrypted using the shared key and re-encrypted using the unique key which is known only to the device itself. The re-encrypted patch program is then stored in nonvolatile memory. Upon reset of the device, the encrypted patch contents are read out of the nonvolatile memory, decrypted using the unique key and loaded into patch memory.